DD/A 75-3375

CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

DD/A Registry
File Security 4-1

17 JUL 1975

Mr. William L. Brown
Executive Director
Interagency Classification Review Committee
National Archives Building
Seventh Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20408

Dear Mr. Brown:

Your 2 July memorandum to Mr. Blake was referred to me for reply.

Please provide the Central Intelligence Agency with 2,100 copies of the pamphlet "Know Your Responsibilities as an Authorized Classifier." Send them directly to the Freedom of Information Coordinator, Central Intelligence Agency, Washington, D.C. 20505. I plan to distribute them, via the Agency's RMO network, to all authorized classifiers, keeping a small supply in reserve.

We welcome the issuance of this pamphlet and trust that it will lead to fuller compliance with the requirements of Executive Order 11652.

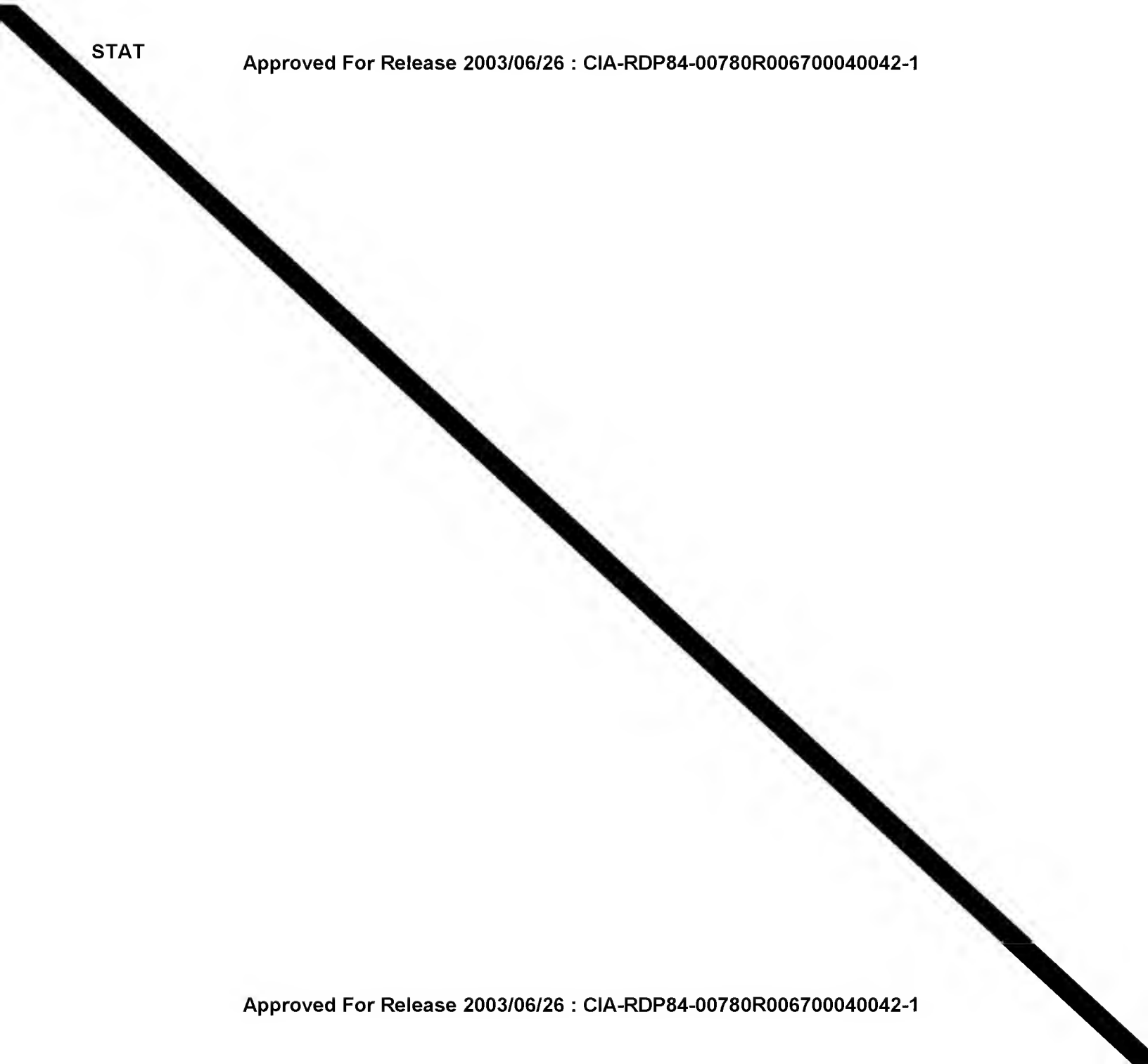
Sincerely,

STAT

Charles E. Savige
Acting Chief, Information Review Staff

IRS:CES:dr (16Jul175)

Distribution:
Original - Addressee
~~1~~ - EO/DDA w/basic
STAT 1 - OGC
1 - ISAS/RAB
1 - IRS Chrono
1 - IRS Subject ~~(w/basic)~~



Approved For Release 2003/06/26 : CIA-RDP84-00780R006700040042-1

INTERAGENCY CLASSIFICATION REVIEW COMMITTEE

WASHINGTON, D.C. 20408

July 2, 1975

MEMORANDUM FOR: JOHN F. BLAKE
CHAIRMAN, DEPARTMENTAL REVIEW COMMITTEE
CENTRAL INTELLIGENCE AGENCY

SUBJECT: ICRC TRAINING PAMPHLET FOR AUTHORIZED CLASSIFIERS

As part of its continuing emphasis on effective orientation and training programs in the security classification field, the Interagency Classification Review Committee has published the enclosed pamphlet entitled "Know Your Responsibilities as an Authorized Classifier." A copy should be given to each employee who has classification authority. Please let us know how many copies your agency will need and to whom they should be sent. There is no charge.

Active and comprehensive orientation and training programs can be one very effective way to prevent abuse of the classification system. Reports to the ICRC reflect that the overwhelming majority of abuses being committed are in the area of improper classification marking, primarily the failure to mark a document with the required stamps or to its assigned classification and as to its assigned declassification schedule or exemption therefrom. To a lesser extent, the other areas of reported abuse are (1) over- or under-classification and (2) the unauthorized use of classification authority. We hope the pamphlet will be a helpful adjunct to your program by helping to eliminate abuse through more active orientation and training.

WILLIAM L. BROWN
Executive Director

STAT

KNOW YOUR RESPONSIBILITIES AS AN AUTHORIZED CLASSIFIER

TOP SECRET

When Classifying a Document

Unless specifically exempted, pursuant to one of the four exemption categories set forth in Section 5(B) of Executive Order 11652, by an official authorized to originally classify information or material TOP SECRET, classified information and material must be subject to the General Declassification Schedule (GDS). Alternatively, it may be designated for automatic declassification on a given event or on a date earlier than provided for in the GDS. This is called the Advance Declassification Schedule (ADS). The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements.

Proper marking of a classified document is important! Each classified document shall show on its face its classification and whether it is subject to the ADS or GDS or exempt from the GDS. Only authorized stamps, properly completed, may be used. If a document is stamped "Restricted Data" or "Formerly Restricted Data," such markings are, in themselves, evidence of exemption from the GDS. The face of the document shall also show the office of origin and the date of preparation and classification. To the extent practicable, the body of the document should be marked to indicate which portions are classified and at what level and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified. Each classified document must also identify in some manner, in accordance with approved procedures, the individual at the highest level that authorized the classification. Where the individual who signs or otherwise authenticates a document has also authorized the classification, no further annotation as to his identity is required. Every authorized classifier should become thoroughly familiar with the proper marking requirements.

If the classifier has any substantial doubt as to which of the classified categories is appropriate, or as to whether the information or material should be classified at all, the least restrictive treatment should be used.

Special Responsibility To Protect

An authorized classifier or other holder of national security information or material shall observe and respect the classification assigned by the originator, giving it the strict protection required by its level of classification. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under Executive Order 11652, the holder shall so inform the originator, who shall thereupon reexamine the classification. Under no circumstances may a holder make an unauthorized release of national security information. There are provisions in the U.S. Criminal Code and other applicable statutes relating to penalties for such unauthorized disclosures.

Implementation and Review Responsibilities

The Interagency Classification Review Committee (ICRC) was established at the direction of the President to assist the National Security Council in monitoring the implementation of Executive Order 11652. The ICRC has extensive oversight responsibilities, which are outlined in the order and in the implementing National Security directive of May 17, 1972.

Within each department or agency, there is a departmental review committee that has responsibilities to act on all suggestions or complaints with respect to the individual department's administration of the order. Such suggestions or complaints may include those regarding over-classification, failure to declassify, or delay in declassifying not otherwise resolved.

Interagency Classification Review Committee
Washington, D.C. 20408

GSA FPC 75-11231

A new system for classifying Government documents relating to national security matters was established on March 8, 1972, by Executive Order 11652 and further implemented by a National Security Council (NSC) directive on May 17, 1972. The change represented the first major overhaul in the classification system of Federal documents in 20 years. Every authorized classifier should obtain a copy of the order, the implementing NSC directive, and the regulations of his or her own department or agency and become thoroughly familiar with their contents.

Authority To Classify

The authority to originally classify information or material under Executive Order 11652 is restricted solely to those offices within the executive branch, enumerated in the order, that are concerned with matters of national security and is limited within those offices to the minimum number of persons absolutely required for efficient administration. This authority may be exercised only by the heads of the departments or agencies and certain other properly designated officials and subordinates. No one else may assign original classifications. Designated officials may classify information or material only at the level authorized and below. Authority to classify may not be delegated to individuals not properly designated.

Security Classification Categories

Official information or material that requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (collectively termed "national security" information or material) shall be classified in one of three categories; namely, TOP SECRET, SECRET, or CONFIDENTIAL. No other categories shall be used except as expressly provided by statute. These categories may only be used in accordance with the following definitions:

TOP SECRET refers to that national security information or material which requires the highest degree of protection. The test for assigning TOP SECRET classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

SECRET refers to that national security information or material which requires a substantial degree of protection. The test for assigning SECRET classification shall be whether its unauthoribed disclosure could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security. The classification SECRET shall be used sparingly.

CONFIDENTIAL refers to that national security information or material which requires protection. The test for assigning CONFIDENTIAL classification shall be whether its unauthoribed disclosure could reasonably be expected to cause damage to the national security.

Other designations coupled with one of the above three categories pertain to access restrictions only.

Personal Responsibility

Each person possessing classifying authority shall be held accountable for the propriety of the classification attributed to him. Both unnecessary classification and over-classification must be avoided. Classifications must be based solely on national security considerations. In no case may information be classified to conceal inefficiency or administrative error, to prevent embarrassment to a person or department, to restrain competition or independent initiative, or to prevent for any other reason the release of information that does not require protection in the interest of national security.

Any Government officer or employee who unnecessarily classifies or over-classifies information or material will be so notified. Repeated abuse of the classification process is grounds for an administrative reprimand. The term "classification abuse" means unnecessary classification, over- or under-classification, failure to assign the proper downgrading and declassification schedule, improper application of classification markings, improper placing of a document in any exempt declassification category, any classification or exemption action taken without authority, or an improper delegation of classification authority.